IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

LALEH NAZ ZAHEDI, a naturalized American citizen of Iranian descent, Plaintiff, v. DEPARTMENT OF JUSTICE; ET AL., Defendants.	)	Civil No. 10-694-JO OPINION AND ORDER

Thomas H. Nelson
THOMAS H. NELSON & ASSOCIATES
20820 E. Glacier View Road
Zigzag, OR 97049

Attorney for Plaintiff

Eric J. Beane
U.S. DEPARTMENT OF JUSTICE
20 Massachusetts Avenue, N.W.
Washington, D.C. 20530

Attorney for Defendants

JONES, Judge:

Plaintiff brings this action for injunctive, declaratory, and monetary relief against the Department of Justice ("DOJ"), the Federal Bureau of Investigation ("FBI"), the Internal Revenue Service ("IRS"), and two individuals, alleging claims under the Privacy Act of 1974, the Freedom of Information Act, and Federal Declaratory Judgment Act.

The case is now before the court on defendants' motion (# 9) to dismiss all claims for failure to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6). For the reasons stated below, defendants' motion is granted and this action is dismissed with prejudice.

STANDARD

A complaint may survive a Rule 12(b)(6) motion to dismiss for failure to state a claim if it contains "'enough facts to state a claim to relief that is plausible on its face.'" Coto Settlement v. Eisenberg, 593 F.3d 1031, 1034 (9th Cir. 2010) (quoting Ashcroft v. Iqbal, ___ U.S. ___, 129 S.Ct. 1937, 1949 (2009)). The court must "construe the complaint in the light most favorable to the plaintiff, taking all her allegations as true and drawing all reasonable inferences from the complaint in her favor." Doe v. United States, 419 F.3d 1058, 1062 (9th Cir. 2005).

PLAINTIFF'S ALLEGATIONS

Plaintiff alleges the following. Plaintiff, of Iranian descent, has been a naturalized American citizen since 2000. After her arrival in the United States in 1994, plaintiff resided at several locations in Ashland, Oregon, and used computers at those locations to create and maintain personal files as well as to communicate with her friends and family, including friends and family in Iran. Some of those communications concerned personal private views on political, religious, social, and family financial matters. Complaint, ¶¶ 11, 12.

Plaintiff alleges that the computers she used were also used by the Qur'an Foundation and later by the Al-Haramain Islamic Foundation in Ashland, Oregon ("AHIF-Oregon"). In February 2004, the computers were located at AHIF-Oregon's building in Ashland, where plaintiff also resided. Complaint, ¶ 13.

On February 13, 2004, the U.S. District Court for the District of Oregon issued a search warrant to the IRS. The warrant authorized a search of AHIF-Oregon's building. Complaint, ¶ 14. Among the items permitted to be seized were computer equipment and storage devices located on the premises. Complaint, ¶¶ 16-17 and Exhibit 1.

In a hearing on July 13, 2009, defendant David Carroll of the FBI acknowledged that in December 2008, the U.S. government had "copied and turned over to Russian intelligence officials of the Federal'naya Sluzhba Bezopasnosti, or 'FSB,' copies of the hard disks seized in February 2004." Complaint, ¶ 19. Plaintiff alleges on information and belief that her "personal and private electronic data, materials and communications, as well as other matters irrelevant to the scope of the search warrant, were contained on the copies of the hard drives provided to the FSB." Complaint, ¶ 20.

Based on the above, plaintiff alleges three claims. In her first claim, titled "Privacy Act/Freedom of Information Act – Denial of Access to Records," plaintiff alleges that she submitted a Freedom of Information Act ("FOIA") request for an accounting of all disclosures of her personal and private electronic data made to the FSB, but no accounting of the disclosures has been forthcoming. Complaint, ¶¶ 24, 25, 27. In her second claim, titled "Privacy Act – Improper Dissemination," plaintiff alleges that the dissemination of information violated her privacy rights both because the government failed to obtain her written authorization before

disseminating the information and because the disclosure was not permitted as a "routine use." Complaint, ¶¶ 31-32. In her third claim, titled "Privacy Act -- Improper Dissemination by Violation of Terms of Search Warrant," plaintiff alleges that the government failed to comply with the terms of the search warrant by retaining and disseminating her private information, and that the government did so "intentionally or willfully in violation of [plaintiff's] privacy rights." Complaint, ¶ 35-37.

DISCUSSION

The following background information, drawn from the Complaint and defendants' Memorandum in Support of Motion to Dismiss, together with the attachments to both, is helpful to an understanding of the issues in this case.

1. Factual and Procedural Background

a. Criminal Search Warrant

As mentioned, in February 2004, the court issued a search warrant authorizing a search of a residential building owned by the Al Haramain Islamic Foundation, Inc. The search warrant listed the individuals associated with possible criminal violations (including Pirouz Sedaghaty, Soliman Al Buthe, Aqeel Al-Aqeel, Mansour Al-Kadi, and Mahmoud Talaat El-Fiki) and the entities associated with violations (including AHIF-Oregon and the Al Haramain headquarters in Riyadh, Saudi Arabia). Complaint, ¶ 14 and Exhibit 1 (search warrant). The search warrant authorized the seizure of "[e]vidence concerning the subscription to a false Form 990 Tax Return, in violation of Title 26, United States Code, Section 7206(1), as described in the attached affidavit, for the year 2000," as well as "[e]vidence relating to the failure to file a currency and monetary instrument reporting form, in violation of Title 31, United States Code, Section 5324."

Search warrant, pp. 5-6. The Affidavit in Support of an Application for Search Warrant, which was incorporated into the search warrant itself, provides further context concerning the criminal investigation, including information about the Al Haramain Islamic Foundation's ties to and financing of global terrorism, including support of the Chechen mujahideen in Russia. See Defendants' Memorandum in Support of Motion to Dismiss, Attachment 1 (Affidavit).

b. Sanctions for Terrorism Financing

On September 8, 2004, the President, through his delegate,[1] designated AHIF-Oregon as a "Specially Designated Global Terrorist" under the Global Terrorism Executive Order No. 13,224 ("E.O. 13,224"), 66 Fed. Reg. 49,079 (2001), and the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1706. Sanctions were imposed on AHIF-Oregon because it was owned or controlled by, or acted for and on behalf of, persons determined to be subject to E.O. 13,224, and because it "assist[ed] in, sponsor[ed], or provide[d] financial, material, or technological support for, or financial or other services to or in support of, such acts of terrorism or those persons listed in the Annex to [E.O. 13,224] or determined to be subject to [E.O. 13,224]." See E.O. 13,224, § 1(d)(I). The United Nations also sanctioned AHIF-Oregon as an "entity belonging to or associated with the Al-Qaida organisation."[2] Defendants' Memorandum, pp. 5-6.

AHIF-Oregon filed an action in this district challenging its designation as a Specially Designated Global Terrorist, but Judge King upheld the government's action and

---

[1] The U.S. Department of the Treasury, Office of Foreign Assets Control.

[2] See "Consolidated List of Individuals and Entities Belonging to or Associated with the Taliban and Al-Qaida Organisation as Established and Maintained by the 1267 Committee," *available at* http://www.un.org/Docs/sc/committees/1267/1267ListEng.htm.

the sanctions remain in place. See Al Haramain Islamic Found., Inc. v. U.S. Dep't of the Treasury, 585 F. Supp. 2d 1233, 1249 (D. Or. 2008) (argued and submitted to the Ninth Circuit March 9, 2011).

2. Plaintiff's Claims

a. Privacy Act/FOIA Request for Accounting

Plaintiff alleges that she has a legal right under the Privacy Act and FOIA to obtain an accounting of all disclosures of her personal and private electronic data, materials and communications contained in the hard drives provided to the FSB. Defendants agree that under section 552a(c)(3) of the Privacy Act, individuals named in records may seek an accounting of disclosures in certain circumstances, but contend that the records at issue here fall squarely within statutory limitations on disclosure. Specifically, defendants rely on the general exemption set forth in section 552a(j)(2) and the specific exemption set forth in section 552a(k)(2). Those exemptions provide in relevant part as follows:

> (j) **General exemptions. --** The head of any agency may promulgate rules . . . to exempt any system of records within the agency from any part of this section [including 552a(c)(3)]. . . if the system of records is--
>
> * * *
>
> (2) . . . (B) information compiled for the purpose of a criminal investigation . . . .

5 U.S.C. § 552a(j)(2)(B). Section 552a(k) further provides specific exemptions, including, as relevant here, an exemption for "investigatory material compiled for law enforcement purposes" in circumstances not covered by the general exemption set forth in subsection (j)(2). 5 U.S.C. § 552a(k)(2).

As required, the DOJ promulgated rules covering these exemptions, identifying an exemption for "Criminal Case Files" (28 C.F.R. § 16.81(a)(1)(4)), and included the necessary statement as to the "reasons why the system of records is to be exempted from a provision of this section [552a]." 5 U.S.C. § 552a(j). That statement explains:

> Exemptions from the particular subsections are justified for the following reasons:
>
> (1) From subsection (c)(3) because the release of the disclosure accounting, for disclosures pursuant to the routine uses published for these systems, would permit the subject of a criminal investigation and/or civil case or matter under investigation, litigation, regulatory or administrative review or action, to obtain valuable information concerning the nature of that investigation, case or matter and present a serious impediment to law enforcement or civil legal activities.

28 C.F.R. § 16.81(b)(1).

As the factual background set forth above clarifies, plaintiff seeks an accounting of information obtained pursuant to a search warrant in the context of a criminal investigation, which falls squarely within the exemptions to the Privacy Act's accounting provision. Although she argues that the material at issue does not qualify as "investigatory material" because her personal records were not listed among the "items to be seized" under the search warrant, plaintiff's argument is not persuasive. While she is correct that the specific evidence described in the search warrant does not mention her personal records, the search warrant plainly authorizes seizure of the computers, including "[a]ny computer equipment and storage device capable of being used to commit, further, or store evidence of the offense[s] listed above." Search Warrant, p. 7. Plaintiff voluntarily put her personal information on computers belonging to a designated terrorist organization and used by Pirouz Sedaghaty, who was convicted of two criminal

violations related to a financial transaction designed to support the Chechen mujahideen in Russia. See generally United States v. Sedaghaty, et al., 2010 WL 1490306 (April 13, 2010)(Hogan, J.). Those computers properly were seized as "investigatory material" and examined under the authority of the search warrant.

Plaintiff further contends that she is entitled to an accounting pursuant to a proviso set forth in section 552a(k)(2). The proviso states:

> *Provided, however*, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual. . . .

5 U.S.C. § 552a (k)(2). Plaintiff's reliance on that provision is misplaced, as she has not identified any right, privilege, or benefit that has been denied to her because of the seizure of her personal records. Moreover, it appears that the original hard drives have been returned to the Al Haramain Islamic Foundation, of which plaintiff's counsel is the current President and sole corporate officer. See Defendants' Reply Memorandum, p. 11. Nothing prevents plaintiff from retrieving any information on the hard drives that pertains to her.

For the above reasons, plaintiff's first claim is dismissed for failure to state a claim.

b. Privacy Act/Improper Dissemination

Plaintiff next alleges that defendants violated the Privacy Act, 5 U.S.C. § 552a(d)(1), by disseminating her private information "to the FSB and unknown others," without receiving her written authorization. Complaint, ¶¶ 31-32.

The Privacy Act governs the acquisition, maintenance, and control of information about individuals by federal agencies. The Act applies only to "records" maintained in a "system of

records" by a federal "agency" that are "retrieved" by the name or other identifying information of the individual. 5 U.S.C. § 552a (definitions). The Act defines "record" as "any item, collection, or grouping of information about an individual that is maintained by an agency. . . ." 5 U.S.C. § 552a(a)(4). "System of records" is defined, in turn, to mean "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).

As a preliminary matter, plaintiff has neither alleged nor established that her "personal and private electronic data, materials and communications" qualify as a "record" or "system of records" within the meaning of the Privacy Act. Even if plaintiff could properly state a claim under § 552a(d)(1), however, she has no claim under the circumstances presented here. As defendants explain in their memorandum:

> In the aftermath of the attacks on the United States on September 11, 2001, Congress twice amended the National Security Act of 1947, first to allow for greater information sharing between law enforcement and intelligence officials, and then explicitly to authorize the disclosure of foreign intelligence information to foreign government officials, notwithstanding any other law. *See* United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act"), Pub. L. No. 107-56, tit. II, § 203(d), 115 Stat. 272, 281 (codified at 50 U.S.C. § 403-5d); Homeland Security Act of 2002, Pub. L. No. 107-296, tit. VIII, § 897(a), 116 Stat. 2135, 2257 (also codified at 50 U.S.C. § 403-5d).

Defendants' Memorandum in Support of Motion to Dismiss, pp. 2-3. 50 U.S.C. § 403-5d(1), in relevant part, authorizes the following:

> Notwithstanding any other provision of law, it shall be lawful for . . . foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official

> receiving that information in the performance of his official duties. . . . [I]t shall be lawful for information revealing a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, obtained as part of a criminal investigation to be disclosed to any appropriate Federal, State, local, or foreign government official for the purpose of preventing or responding to such a threat.

(Emphasis added.) Included within the definition of "foreign intelligence information" is "information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—(I) the national defense or the security of the United States; or (ii) the conduct of the foreign affairs of the United States." Id. § 403-5d(2).

It is beyond dispute that the computer hard drives, as described in Judge Hogan's Order in the related criminal case, contained "foreign intelligence information:"

> In a joint effort to fight terrorism, the United States and the Russian Federation exchange information and evidence concerning the activities of Al Haramain. The information exchange at issue apparently took place in 2008.
>
> The two countries are parties to a treaty requiring exchange of information. At a December 2008 meeting, representatives of the Russian FSB provided the United States with certain evidence relevant to this prosecution, as requested by the United States under the Treaty. For example, the Russian FSB disclosed that it had learned that Al Haramain had smuggled money into Chechnya through an Al Haramain office in Baku, Azerbaijan. Some of this money was funneled to the Kavkaz Islamic Institute, which was a training camp for the mujahideen in Chechnya. The money from this so-called charity was used "to purchase weapons, uniforms, medicine, communication devices, vehicles, and to pay religious extremists' salaries."
>
> * * *
>
> At this December 2008 meeting, U.S. law enforcement provided a copy of the computer hard drives seized from Al Haramain USA in Oregon pursuant to the warrant. Those hard drives contained substantial evidence of interest to the Russian government in its on-going efforts to counter terrorism in the Caucasus.

> For example, the Al Haramain USA hard drives contained the photographs of captured and dead Russian soldiers, as well as photographs of some of their identity papers. It is understandable that Russia might have an interest in examining the Al Haramain USA computers to account for its own soldiers. Other information relevant to jihads in Chechnya from the computers were provided.

United States v. Sedaghaty, et al., 2010 WL 1490306 at *10 (footnote omitted); see also Al Haramain Islamic Found., Inc. v. U.S. Dep't of the Treasury, 585 F.Supp. at 1252 and n.9.

Further, although the Privacy Act generally provides that "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency," the Act does not prohibit disclosure of an agency record if the disclosure is made pursuant to an established "routine use." 5 U.S.C. § 552a(b)(3). "Routine use" means "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(a)(7). Agencies are required to publish in the Federal Register "each routine use of the records contained in the system, including the categories of users and the purpose of such use." 5 U.S.C. § 552a(e)(4)(D).

As defendants concisely explain,

> Both the IRS and FBI have published a routine use in the Federal Register that covers the present circumstances and forecloses any factual question about whether, assuming the facts alleged in Plaintiff's Complaint are true, the Privacy Act has been violated.
>
> The seized records, including the "copy of the hard drives" referenced in Plaintiff's complaint, fall within the Department of the Treasury/Internal Revenue Service System of Records 42.013. *See* Privacy Act of 1974, as Amended; System of Records, 73 Fed. Reg. 13,284, 13,333-35 (March 12, 2008). The IRS criminal investigation that Plaintiff references pertains to Titles 26 and 31 of the United States Code. The Title 26 investigation was related to filing a false federal tax Form 990 for year 2000, and the Title 31 investigation related to a failure to file Currency or Monetary Instruments. Included within Treasury/IRS System of Records 42.031 "category of records" are records relating to the administration of

> the IRS's anti-money laundering program including the registration, reporting, and record-keeping requirements of the Bank Secrecy Act.

Defendants' Memorandum in Support of Motion to Dismiss, p. 16. The "routine uses" of records maintained in System of Records 42.031 specify that it is appropriate to:

> [d]isclose information to appropriate Federal, State, local or foreign agencies responsible for investigating or prosecuting the violations of or for enforcing or implementing a statute, rule, regulation, order, or license, where the Service becomes aware of an indication of a potential violation of civil or criminal law or regulation, or the use is required in the conduct of intelligence or counter-intelligence activities, including analysis, to protect against international terrorism.

73 Fed. Reg. at 13,334; see also the FBI's published "routine use" covering systems of records containing investigatory files, System of Records, 66 Fed. Reg. 33,558, 33,559 (June 22, 2001)(Blanket Routine Use ## 1, 6).

In sum, plaintiff's second claim, for improper dissemination, fails both because the disclosure was authorized by statute and because the dissemination falls within the published routine uses of the IRS and FBI.

c. Violation of Search Warrant

Plaintiff next alleges a Privacy Act claim based on violation of the terms of the search warrant. Defendants correctly point out that the Privacy Act does not create a cause of action for such a violation, a point plaintiff evidently concedes. See Plaintiff's Response to Defendant's Motion to Dismiss, p. 13. Instead, plaintiff discusses the parameters of her claim as if she had alleged it under Bivens v. Six Unknown Named Agents, 403 U.S. 388 (1971). Plaintiff has not, however, alleged a Bivens claim in this case, something she apparently acknowledges as evidenced by her recent filing of a separate Bivens complaint in Zahedi v. Anderson, et al.,

CV No. 11-446-JO. The viability of plaintiff's claims in that action is not presently before the court, but plaintiff's Privacy Act claim for violation of the terms of the search warrant in this action is not valid.

In summary, defendants' motion to dismiss plaintiff's complaint is well-taken and is granted in full. That plaintiff's personal information was "swept up in the dragnet of all computer records seized"[3] from the headquarters of a "Specially Designated Global Terrorist" in the context of an investigation of the illicit financing of global terrorism, including support of the Chechen mujahideen in Russia, and disclosed to the FSB may be unfortunate for her, but is not actionable under the Privacy Act in view of the Patriot Act and Homeland Security Act amendments to the National Security Act of 1947.

CONCLUSION

Defendants' motion (# 9) to dismiss is GRANTED and this action is dismissed with prejudice. Any other pending motions are denied as moot.

DATED this 16th day of May, 2011.

/s/ Robert E. Jones
ROBERT E. JONES
U.S. District Judge

[3] Plaintiff's Response to Defendants' Motion to Dismiss, p. 12.